INCIDENT REPORT

Date & Time Reported to ITOC:	
Agency:	
Reported by: ▪ **Name** ▪ **Phone** ▪ **E-mail**	
Nature of Incident: ☐**Denial of Service** ☐**Malicious Code** ☐**Reconnaissance Scans and Probes** ☐**Unauthorized Access** ☐**Other (describe)**	
Location of Affected Systems: ▪ **Address** ▪ **Building/Room**	
Details: (virus name, events, etc)	
Date & Time Occurred:	
Date & Time Detected:	
How was the Incident detected?	
Describe overall business impact of incident:	
Compromised System Details	
System(s) affected ▪ **Host/node name** ▪ **Network address**	
Hardware involved ▪ **Manufacturer** ▪ **Model**	
O/S ▪ **Version** ▪ **Patch level**	
Compromised account name(s) ▪ **Version** ▪ **Patch level**	
Compromised software	
Source of attack	
Describe What Actions have been taken so far	
Was system removed from network?	
Audit logs recovered and examined?	

INCIDENT REPORT

Which?	
Forensic backups made? **Original media secured?**	
Describe initial containment measures (firewall, ACL, etc)	
Who has been notified? (e.g. ISP? State Police?) **When notified** ▪ **Date and time**	
Technical contact (System/network administrators)	
Additional Information:	